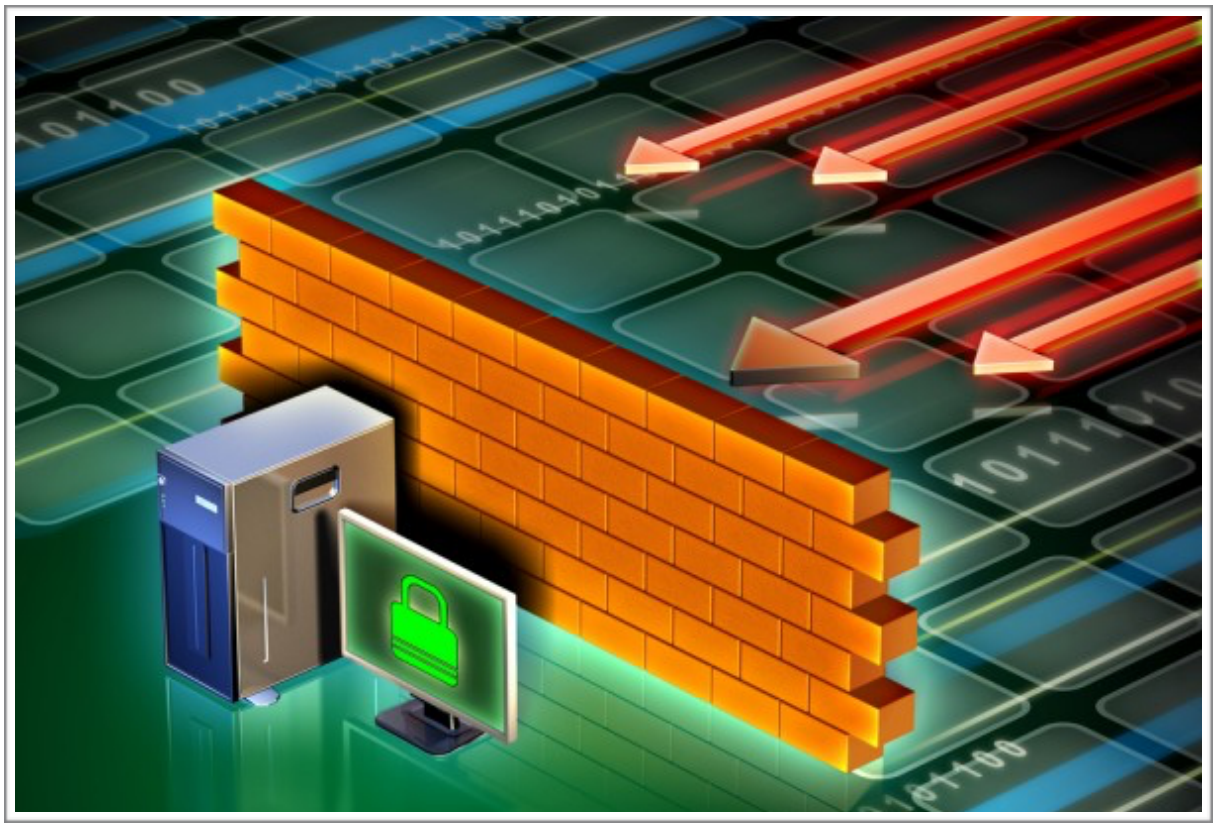
白山云CC防火墙产品说明



白山云科技

2016.8

产品简介

CC防火墙是白山云科技（简称：白山）下云聚合产品中的子产品，目的是为企业提供针对Challenge Collapsar Attack（简称：CC攻击）的防火墙产品，本防火墙可有效的防范各种HTTP攻击，预计防护能力达到1000,000 rps，并具备自学习能力，可以预防变种攻击。本防火墙同时支持公有云和私有云两种部署模式，私有云部署模式不依赖特殊硬件，可以在任何Linux Server上运行。

产品功能和特点

白山CC防火墙不同于传统的硬件防火墙的简单策略机制，而是利用了大数据计算模型收集访问日志，进行实时计算，进行行为学习和归类，最终将判定结果反馈到拦截模块。拦截模块不同于一般的外层负载均衡拦截模式，而是在Linux内核态直接拦截，比传统的负载均衡拦截性能快一个数量级。同时，CC防火墙还支持分域名拦截，可以实现同一个IP在某一个域名下拦截，而在别的域名下不拦截。另外，CC防火墙对于拦截可以分轻重进行，轻粒度的可以拦截后自动跳转到验证码页面，对于重粒度行为则直接进行包drop，提高攻击者的攻击成本。

白山CC防火墙的功能列表：

识别	自定义日志推送
	实时分析
	自定义识别规则
拦截	分域名拦截
	内核拦截
	灰IP自动跳转验证码
	自定义拦截行为

白山CC防火墙可识别的攻击类型：

负载消耗攻击	HTTP flood

CPU消耗攻击	随机构造攻击
	404穿透攻击
连接数消耗攻击	HTTP发包慢速攻击
	HTTP收包慢速攻击
流量消耗攻击	异常header包攻击
	异常body包攻击
其他	高频验证码校验
	经验抓站UA

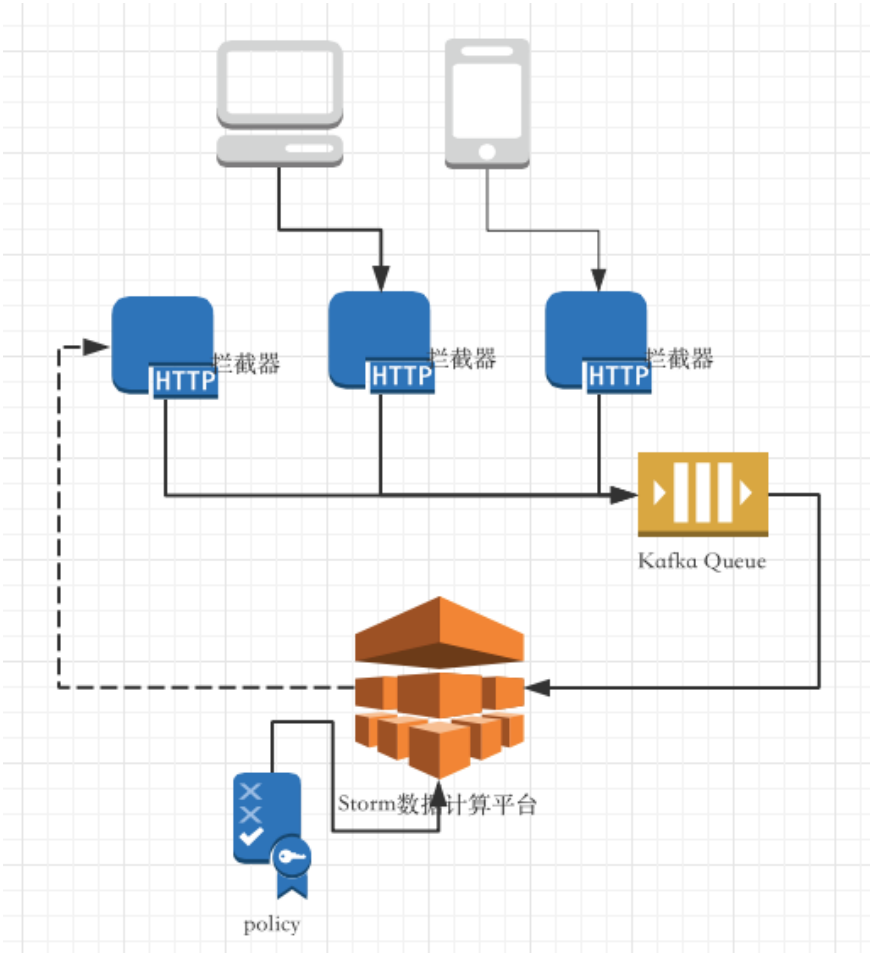
白山CC防火墙性能指标

部署环境	10台* 24核 128G内存 Centos 6.5
每分钟处理请求数	6000万

对比友商，白山CC防火墙特点：

架构特点	公有云/私有云部署	白山云云聚合同时支持公有云、私有云两种部署模式，企业既可以使用白山云聚合公有云服务，对于某些安全性要求高的企业，又可以快速的将云聚合产品部署在企业内部
	软件实现	白山云聚合可以部署在任意Linux架构的服务器上，不依赖特殊硬件，基于通用开源软件，方便部署/维护，不存在绑定关系
技术特点：	无状态对等部署	采用无状态对等部署，没有单点，保证服务高可靠性
	防火墙内核拦截技术	不同于传统的7层防火墙，白山云HTTP防火墙具有3层拦截技术，工作在Linux Kernel网络栈，性能比7层防火墙高一个数量级
	流式大数据分析	基于Storm流式实时大数据分析，可以几秒内即做出分析响应
	防火墙防误拦技术	针对公司上网时，同一个出口IP产生大量的正常访问行为这种情况，白山云拥有一套基于用户特征分布模式的算法分析，可以区别出攻击行为还是正常行为，最终提供准确拦截
	包丢弃技术	传统的7层防火墙的返回HTTP错误码或者RST拦截从本质上来讲并没有增加攻击者的攻击成本，而白山云HTTP防火墙使用独有的包丢弃技术，拦截攻击IP后，攻击者会发生超时现象，大大增加攻击者的攻击成本

实现原理



如图所示:

白山CC防火墙主要由3个模块组成:

1，拦截器（可选），拦截器主要起到在内核层拦截攻击包的作用，性能是应用层拦截的10倍以上，当然用户如果自行有拦截机制，可以不安装此模块

2，Kafka队列，用于收集HTTP请求日志，进行缓存和高效的读取

3，Storm大数据计算平台，用于将实时收集的HTTP请求日志进行分析，内置了核心分析和学习算法，可以识别多种类型的攻击。

总体的工作流程为:

1，将HTTP访问请求日志写入kafka队列

2，大数据分析平台通过kafka队列读取实时用户请求，进行算法分析，得出结果：攻击类型、攻击IP、应对策略

4，根据相应的应对策略进行不同程度的拦截

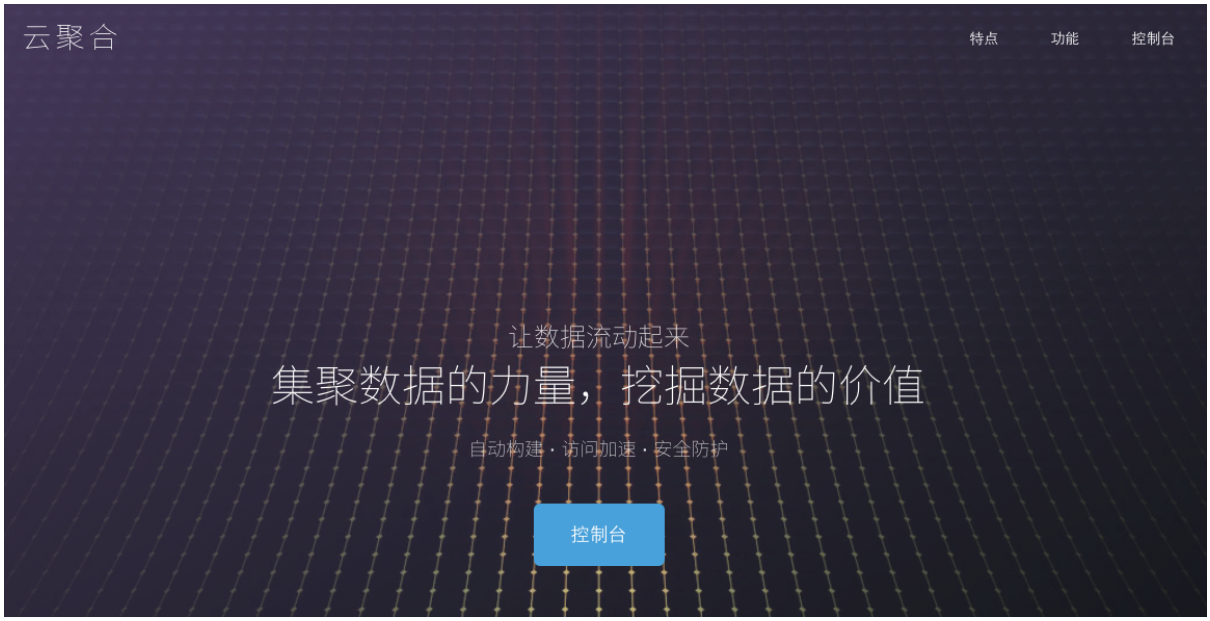
产品使用

白山CC防火墙有两种部署使用模式：

A，公有云部署

用户直接使用白山部署在公网上的云聚合服务，对接自己的业务后端（需要保护的对象），然后将自己的域名cname到白山生成的域名（*.bsclink.com）即可。

步骤1，登陆白山云云聚合首页，进入控制台

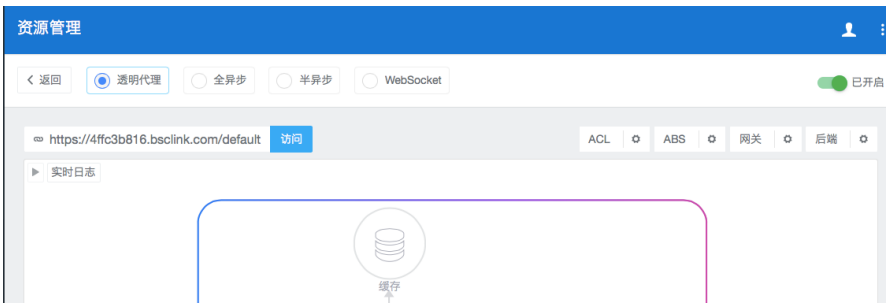


步骤2，创建一个API

步骤3，添加后端（以百度网站为例 baidu.com）

步骤4，配置安全中心（打开防火墙，具体配置请和技术支持沟通后进行）

步骤5，开启该应用

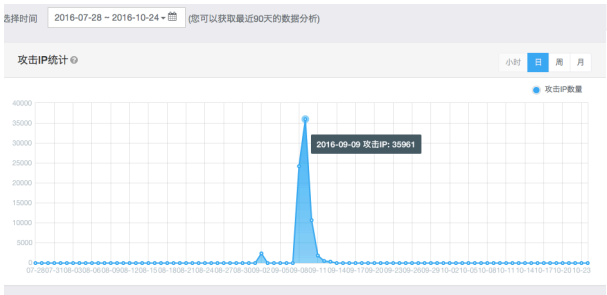


步骤6，此时访问即可见到效果：

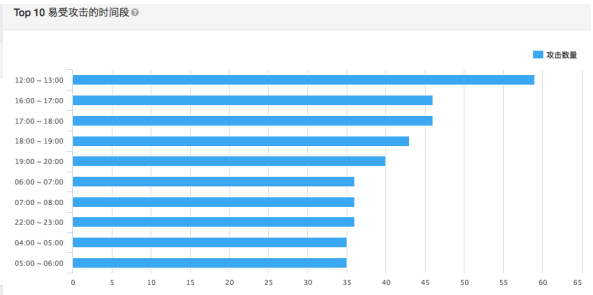
```
[conglei@iZ25ji98i3hZ ~]$ ab -c 200 -t 30 http://4ffc3b816.bsclink.com/default
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 4ffc3b816.bsclink.com (be patient)
apr_poll: The timeout specified has expired (70007)
```

步骤7：查看拦截结果展现（数量、时间段、地域、原因分析、详情展示）

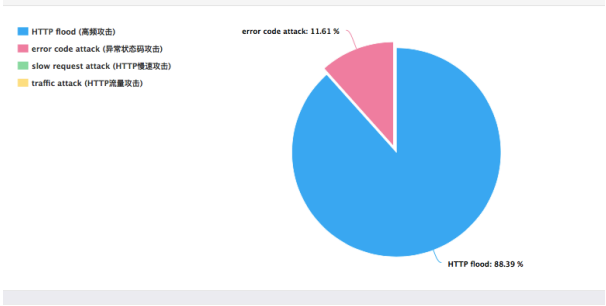


时间	攻击IP数量
09-19	2
09-14	1
09-13	351

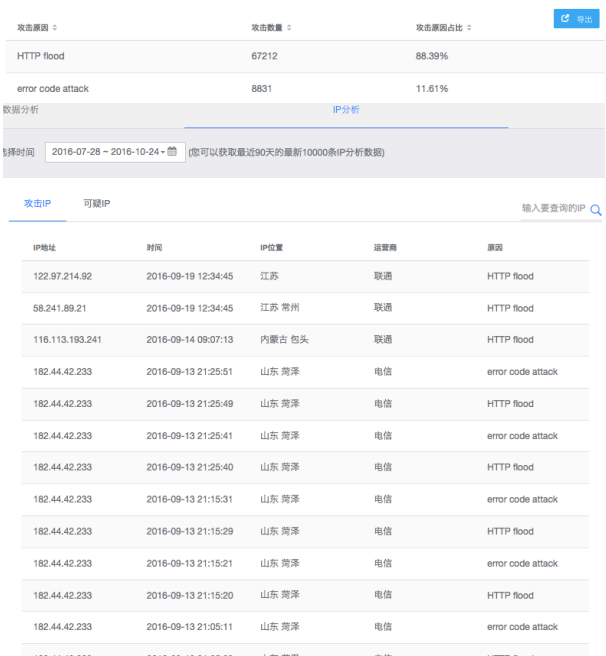


被攻击的时间段	攻击数量	攻击占比
12:00 ~ 13:00	59	6.83%
16:00 ~ 17:00	46	5.32%
17:00 ~ 18:00	46	5.32%

省份	攻击IP数量	攻击占比
广东	31502	41.43%
浙江	23664	31.12%
云南	13704	18.02%



攻击原因	攻击数量	攻击原因占比
HTTP flood	67212	88.39%
error code attack	8831	11.61%



IP地址	时间	IP位置	运营商	原因
122.97.214.92	2016-09-19 12:34:45	江苏	联通	HTTP flood
58.241.89.21	2016-09-19 12:34:45	江苏 常州	联通	HTTP flood
116.113.193.241	2016-09-14 09:07:13	内蒙古 包头	联通	HTTP flood
182.44.42.233	2016-09-13 21:25:51	山东 菏泽	电信	error code attack
182.44.42.233	2016-09-13 21:25:49	山东 菏泽	电信	HTTP flood
182.44.42.233	2016-09-13 21:25:41	山东 菏泽	电信	error code attack
182.44.42.233	2016-09-13 21:25:40	山东 菏泽	电信	HTTP flood
182.44.42.233	2016-09-13 21:15:31	山东 菏泽	电信	error code attack
182.44.42.233	2016-09-13 21:15:29	山东 菏泽	电信	HTTP flood
182.44.42.233	2016-09-13 21:15:21	山东 菏泽	电信	error code attack
182.44.42.233	2016-09-13 21:15:20	山东 菏泽	电信	HTTP flood
182.44.42.233	2016-09-13 21:05:11	山东 菏泽	电信	error code attack

云聚合

B，私有云部署模式

私有云部署模式，适用于要求分析过程都在内网进行的企业，部署过程很简单：

1，对于开通外网SSH登陆的企业，我们利用程序部署即可

2，对于无法开通SSH登陆的企业，我们进行上面部署调试

需要部署的模块：

1，Storm大数据技术平台

2，Kafka队列

3，Linux内核拦截模块（可选），如果企业使用特殊的硬件设备（如F5），可以对接接口进行拦截，这样可以不安装此模块

软件环境要求：

Linux Kernel 2.6.32以上，推荐操作系统CentOS 6.2以上，3台机器以上

产品定价

公有云模式：

白山CC防火墙采用专属部署模式（即每个企业在公有云上实际进行隔离部署），按照防护能力进行收费

初级防护	峰值攻击，2万请求/秒	15万RMB/年
中级防护	峰值攻击，10万请求/秒	30万RMB/年
高级防护	峰值攻击，100万请求/秒	100万RMB/年
自定义防护	自定义	销售咨询

私有云模式：

可以部署在企业内部，按照部署规模进行收费

6000RMB/CPU核/年	最小部署单元：3台物理机

Faq

*** 市面上那么多防火墙，我为什么需要使用白山CC防火墙?**

白山CC防火墙是市面上唯一专著于防护CC攻击的防火墙，CC攻击不同于一般的DDoS工具，具有真实IP、行为界定困难、攻击变种多等特点，白山CC防火墙将大数据技术和攻击分析结合起来，并且利用特有的拦截技术进行针对于CC攻击的防护，可以有效的防止恶意抓站、穿透恶意消耗、HTTP慢速攻击等行为。值得一提的是，白山CC防火墙有一套独特的拦截技术，可以对域名进行区分拦截，并且性能比传统的负载均衡拦截快1个数量级。总之，白山云CC防火墙具有几个独有特点：

- 支持私有云部署
- 独有旁路拦截技术，不用串行流量即实现拦截
- 零误拦（深度结合业务特点）
- 包丢弃技术，以大大增加攻击者成本

*** 为什么说CC攻击更加难以防范**

首先，CC攻击都是合法的HTTP请求，都是真实IP，所以在前面的流量清洗设备无法将其拦截。其次，对于高频攻击而言，恶意攻击和群体“秒杀”等行为区别很困难，不进行智能趋势分析不可能进行精准识别。另外，传统的硬件HTTP防火墙在防范CC攻击方面具有明显劣势，比如一些硬件防火墙会利用RST反弹等技术进行防护，但这种技术实际会影响用户体验。最后，CC攻击的变化有很多，用户可以根据实际的请求模式，变化出很多的攻击方式，使人难以防护。

*** 白山CC防火墙可以防syn-flood等流量攻击吗?**

不能，白山CC防火墙专著于防范CC攻击，换句话说，它是工作在入口流量后的，可以有效的防止负载均衡或者Web服务器的CPU、内存、连接数等资源被消耗。但是，如果入口流量被打满，CC防火墙将无法知晓，这种情况请企业购买流量清洗中心进行防御。

*** 大数据分析的延迟有多少?**

经过我们测试，延迟在5秒以内，当然，对于私有云部署模式，这依赖于企业内网通信的延迟和稳定性。

*** 云聚合和CC防火墙是什么关系?**

云聚合是白山云科技推出的针对数据挖掘、接口构建、接口适配、接口加速、接口防护的一整套产品，CC防火墙是云聚合的一个子产品。

*** 私有云部署的话，怎么对接CC防火墙?**

对接CC防火墙只需要做两个工作:

1，将HTTP访问日志推送给Kafka队列，可以使用各种语言的客户端

2，将大数据的分析结果触发到拦截器，如果使用我们自带的拦截器，这块无需关注。但对于某些场景，比如硬件负载均衡，无法部署我们的拦截器，这种情况可以直接对接负载均衡设备的接口，进行拦截。

*** 我们机房环境内部有多层负载均衡，客户源IP怎么传递?**

可以使用HTTP标准header：x-forward-for记录原始客户端IP，也可以使用自定义的标准，总之只要能让CC防火墙知道哪个字段能表示客户端原始IP即可。